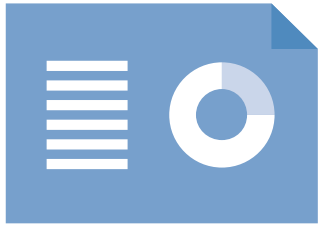
Fireproof Studios

Age Appropriate Design Code Audit Report

April 2022

Executive summary



Background & Scope

Under section 123(1) of the Data Protection Act 2018 (DPA18), the Information Commissioner produced a code of practice on standards of age appropriate design ("the Code"). The Code applies to "relevant information society services which are likely to be accessed by children" in the UK. This includes many apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news or educational websites and websites offering other goods or services to users over the internet. It is not restricted to services specifically directed at children.

The Code sets out 15 headline standards of age appropriate design that companies need to implement to ensure their services appropriately safeguard children's personal data and process children's personal data fairly. The Code came into force on 2 September 2021.

More widely, the Information Commissioner is also responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UKGDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

Fireproof Studios (Fireproof) agreed to a consensual audit of the measures, processes and policies they have in place to demonstrate conformance with the Code and data protection legislation.

The purpose of the audit is to provide the ICO and Fireproof with an independent assurance of the extent to which Fireproof, within the scope of this agreed audit, is complying with data protection legislation.

The scope areas covered by this audit are determined following a risk based analysis of Fireproof's processing of children's personal data. The scope may take into account any data protection issues or risks which are specific to Fireproof, identified from ICO intelligence or Fireproof's own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the

organisational structure of Fireproof, the nature and extent of Fireproof's processing of children's personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to Fireproof.

It was agreed that the audit would focus on the following area(s):

- A: Governance, Transparency and Rights
- B: Diligence and Data Protection Impact Assessments (DPIAs)
- C: Minimisation and Sharing
- D: Age Assurance
- E: Detrimental Use
- F: Privacy Settings and Controls
- G: Geolocation tracking
- H: Profiling and Cookies
- I: Nudge Techniques
- J: Connected Toys and Devices
- K: AI Online Services

Audits are conducted following the Information Commissioner's audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore Fireproof agreed to conduct the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 14 to 17 March 2022. The ICO would like to thank Fireproof for its flexibility and commitment to the audit during difficult and challenging circumstances.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate conformance with the Code and data protection legislation. In order to assist Fireproof in implementing the recommendations each has been assigned a priority rating based upon the risks to children that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. Fireproof's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Overview of Service and Processing

Fireproof Studios are a gaming company and were founded in 2008. Fireproof have 21 staff and are headquartered in Guildford, Surrey.

Fireproof Studios have produced a number of games primarily centred around the series 'The Room'. These games are available on multiple platforms including mobile, PC and more recently Virtual Reality (VR). 'The Room' series is centred around solving 3D puzzles to progress through a storyline, which is split into chapters.

'The Room' game series has received a PEGI 7+ rating for all titles, but Fireproof recommend that children who wish to play the games seek the permission of a parent. This is especially relevant for The Room VR, as VR technology is not recommended for children under 13 years of age. These recommendations are made by VR hardware companies, rather than Fireproof themselves. Fireproof's games are available for purchase on major content stores, such as Apple Arcade, Steam and Oculus. Fireproof do not sell their games directly and do not conduct any direct marketing.

Fireproof has an ethos to put player experience at the heart of their games and has vocalised their desire to produce high quality experiences for players over the collection and processing of personal data. As a result, Fireproof have adopted a privacy-by-design approach when creating their game series 'The Room'. Fireproof do not process personal information in-game and have limited the collection of personal data to when it is necessary to provide a customer support function to children and other users. Fireproof have made deliberate design choices to not make use of dark nudge techniques, not to profile users and to not include in-game content that is likely to be detrimental to children. This has facilitated compliance with many of the Code's standards and as a result children are afforded a high level of protection when interacting with Fireproof's games.

Fireproof process personal data when providing customer support. The information gathered for the purposes of providing support cannot be linked to any in-game information gathered by Fireproof, such as length of session.

Fireproof have developed and made available an End User Licence Agreement (EULA) which sets out a number of permitted and prohibited activities when interacting with Fireproof's games. Users, including children, are given an opportunity to read the EULA before purchase and the EULA, as well as the privacy notice, is available in almost all content stores where the games can be purchased.

Audit Summary

Scope area	Assurance Rating	Overall Opinion
Governance, Transparency & Rights	Reasonable	There is a reasonable level of assurance that processes and procedures are in place, that the organisation is in conformance with the AADC and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-conformance with both the AADC and data protection legislation.
Due Diligence & DPIAs	Reasonable	
Minimisation & Sharing	High	There is a high level of assurance that processes and procedures are in place, that the organisation is in conformance with the AADC and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-conformance with AADC and data protection legislation.
Age Assurance	High	
Detrimental Use	High	
Privacy Settings & Parental Controls	High	
Geolocation	High	
Profiling & Cookies	High	
Nudge Techniques	High	
Connected Toys & Devices	High	
AI Online Services	High	

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

Areas for Improvement

Identify and document a lawful basis for processing and condition for processing special category data. Ensure privacy information is updated to reflect the identified lawful basis and the rights available to children.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the engagement and are not necessarily a comprehensive statement of all the areas requiring improvement. The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Fireproof Studios.

We take all reasonable care to ensure that our report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is solely for the use of Fireproof Studios. The scope areas and controls covered have been tailored to this engagement and, as a result, the report is not intended to be used in comparison with other ICO report.